UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI

SHANNON SMITH, on behalf of himself and all others similarly situated, Plaintiff, v. **CERNER CORPORATION D/B/A ORACLE HEALTH, INC**. and **UNION HEALTH SYSTEM, INC**., Defendants.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Shannon Smith ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Cerner Corporation d/b/a Oracle Health ("Oracle" or "Defendant") and Union Health System, Inc. ("Union Health" or "Defendant") (together "Defendants"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data.

2. Defendant Union Health is a healthcare provider—and Defendant Oracle is a third-party vendor that provides data migration services to Union Health.[1]

3. As such, Defendants stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its

[1] *See* Exhibit B ("Ex. B").

current and former patients. But Defendants lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendants' network before the breach was discovered. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendants' failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice—attached as **Exhibit A**.

7. The breach notice posted on Union Health's website is attached as **Exhibit B** (the notice has since been removed from Union Health's website but is still available via the internet archive).[2]

8. He brings this class action on behalf of himself, and all others harmed by Defendants' misconduct.

9. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former patients' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

---

[2] *See Notice of Oracle Health/Cerner Data Security Incident*, UNION HEALTH (April 21, 2025) https://web.archive.org/web/20250425172754/https://www.union.health/news/noticeoforaclehealthcernerdatasecurityincident .

PARTIES

10. Plaintiff, Shannon Smith, is a natural person and citizen of Terre Haute, Indiana where he intends to remain.

11. Defendant, Cerner Corporation d/b/a Oracle Health is corporation incorporated in Delaware and with its principal place of business at 8779 Hillcrest Road, Kansas City, Missouri 64138.

12. Defendant, Union Health System, Inc., is a corporation incorporated in Indiana and with its principal place of business at 1606 North 7th Street, Terre Haute, Indiana.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendants are citizens of different states. And there are over 100 putative Class Members.

14. This Court has personal jurisdiction because Oracle is headquartered in Missouri, regularly conducts business in Missouri, and has sufficient minimum contacts in Missouri.

15. Venue is proper in this Court because Oracle's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendants Collected and Stored the PII/PHI of Plaintiff and the Class

16. Defendant Union Health is a healthcare provider—and Defendant Oracle is a third-party vendor that provides data migration services to Union Health.[3]

[3] *See* Exhibit B ("Ex. B").

17. As part of its business, Defendants receives and maintains the PII/PHI of thousands of its current and former patients.

18. In collecting and maintaining the PII/PHI, Defendants agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII/PHI.

19. Under state and federal law, businesses like Defendants have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

20. Defendants recognize these duties. For example, Union Health declares in its "Union Health's HIPAA Privacy and Security Plan 2024" that:

a. "It is Union Health's responsibility to comply fully with all HIPAA regulations and to ensure the privacy and security of all forms of PHI."[4]

b. "Union Health has implemented the appropriate administrative, technical, and physical safeguards to protect the privacy of PHI."[5]

c. "The Secretary of Health and Human Services will be notified in the event of a breach of unsecured PHI that affects five hundred or more individuals. The notification will be done without reasonable delay, and no later than 60 days following the discovery of the breach."[6]

d. "A breach of unsecured PHI involving more than five hundred residents of a State or jurisdiction, Union Health will notify prominent media outlets serving the State or jurisdiction. This media notification will be provided

[4] *Union Health's HIPAA Privacy and Security Plan 2024*, UNION HEALTH (Oct. 24, 2024) https://www.union.health/upload/docs/UnionHealth/compliance/HIPAA%20Privacy%20and%20Security%20Plan.pdf.
[5] *Id*.
[6] *Id*.

without reasonable delay and no later than 60 days following the discovery of the breach and should include the same information as the individual notices."[7]

e. "Following the discovery of a breach of unsecured PHI, Union Health shall notify each individual that their unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such breach. This notification will be in plain language and provided without reasonable delay and in no case later than sixty calendar days after the discovery of the breach."[8]

f. "A business associate is an entity that, on behalf of Union Health, but other than the capacity of a member of the workforce: creates, receives, maintains, or transmits PHI for a function or activity including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing[.]"[9]

g. "The business associate may not use or disclose PHI in a manner that would violate HIPAA, if done by the covered entity, or violate the terms of the business associate contract or other assurance."[10]

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

h. "Before disclosing PHI to a business associate, Union Health will obtain satisfactory assurances that the business associate will implement safeguards as required under HIPAA."[11]

i. "A contract between Union Health and a business associate will contain several different elements including language that establishes permitted and required uses and disclosures of PHI by the business associate and ensures that the business associate will not use or further disclose the protected health information[.]"[12]

Defendants' Data Breach

21. On January 22, 2025, Defendants were hacked in the Data Breach.[13]

22. Worryingly, Defendants already admitted that:

a. "An unknown party contacted Union Health claiming they had some patient information in their possession, which we verified on February 24, 2025."[14]

b. "Union Health then identified the information as likely relating to data migration services performed by Oracle Health/Cerner[.]"[15]

c. "On March 15, 2025, Oracle Health/Cerner informed Union Health that it did have a cybersecurity event involving unauthorized access to data hosted in Oracle Health/Cerner's data migration environment."[16]

[11] *Id*.
[12] *Id*.
[13] Ex. B.
[14] *Id*.
[15] *Id*.
[16] *Id*.

d. "Oracle Health/Cerner further informed us that, on February 20, 2025, they first became aware of the incident and that their investigation identified the unauthorized party's initial access as taking place sometime after January 22, 2025."[17]

e. "On March 22, 2025, Oracle Health/Cerner provided us with a list of Union Health patients whose information was involved."[18]

23. Because of Defendants' Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. Social Security numbers;

c. driver's license numbers;

d. dates of birth;

e. treating physicians;

f. dates of service;

g. medication information;

h. insurance information;

i. medical treatment information; and

j. medical diagnostic information.[19]

24. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendants'

[17] *Id*.
[18] *Id*.
[19] *Id*.

custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former patients.

25. And yet, Defendants waited over until April 21, 2025, before it began notifying the class—a full 89 days after the Data Breach began.

26. Thus, Defendants kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

27. And when Defendants did notify Plaintiff and the Class of the Data Breach, Defendants acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "[R]eview statements they receive related to their healthcare provider or health insurer."[20]

28. Defendants failed their duties when their inadequate security practices caused the Data Breach. In other words, Defendants' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendants caused widespread injury and monetary damages.

29. Since the breach, Defendant Union Health claims that "[w]e remain committed to upholding high standards of custodianship of Union Health information held by our third-party vendors, including Oracle Health/Cerner."[21]

30. But such simple declarations are insufficient to ensure that Plaintiff's and Class Members' PII/PHI will be protected from additional exposure in a subsequent data breach.

[20] *Id.*
[21] *Id.*

31. Further, the Notice of Data Breach shows that Defendants cannot—or will not—determine the full scope of the Data Breach, as Defendants has been unable to determine precisely what information was stolen and when.

32. Defendants has done little to remedy its Data Breach. True, Defendants has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendants inflicted upon them.

33. Because of Defendants' Data Breach, the sensitive PII/PHI of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Defendant's Pattern of Negligent Data Practices

34. Worryingly, this Data Breach is only part and parcel of Union Health's pattern and practice of negligence data practices—indeed, in March 2023, Union Health experienced another data breach wherein "an unauthorized party gained access" and "acquired copies of certain files" which included the names, addresses, phone numbers, dates of birth, medical record numbers, and certain health information and Union Health's current and former patients.[22]

Cybercriminals & the Dark Web

35. To make matters worse, third-parties have reported that "impacted hospitals are now being extorted by a threat actor named 'Andrew,' who has not claimed affiliation with extortion or ransomware groups" and that "[t]he threat actor is demanding millions of dollars in

[22] Annie Johnston, *Some Union Health patients impacted by cyber breach at third-party company*, WTHI-TV10 (Dec. 6, 2023) https://www.wthitv.com/news/some-union-health-patients-impacted-by-cyber-breach-at-third-party-company/article_f052250a-9463-11ee-81e4-7790b8f2df68.html.

cryptocurrency not to leak or sell the stolen data and has created clearnet websites about the breach to pressure the hospitals into paying the ransom."[23]

36. This massive Data Breach has been revealed just a few days after it became known that another cybercriminal known as "rose87168" has accessed Oracle Cloud's "federated login infrastructure" and allegedly stolen approximately 6 million sensitive records potentially affecting more than 140,000 Oracle Cloud tenants worldwide.[24]

37. Oracle has been denying both breaches despite hackers offering proof of the sensitive data exfiltrated from Oracle's networks and/or servers, intentionally and/or negligently leaving millions of customers at risk.[25]

38. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[26]

39. Thus, on information and belief, Plaintiff's and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff's Experiences and Injuries

---

[23] Sergiu Gatlan, *Oracle privately confirms Cloud breach to customers*, BLEEPING COMPUTER (April 3, 2025) https://www.bleepingcomputer.com/news/security/oracle-privately-confirms-cloud-breach-to-customers/.

[24] Brian Rankin, *Oracle Health Breach: What Life Sciences Cybersecurity Leaders Need to Know—and Do—Now*, USDM LIFE SCIENCES (April 2, 2025) https://usdm.com/resources/blogs/oracle-health-breach-what-life-sciences-cybersecurity-leaders-need-to-know-and-do-now.

[25] Ellen Jennings-Trace, *Oracle Health suffers major breach, hospital data potentially exposed*, TECH RADAR (March 31, 2025) https://www.techradar.com/pro/security/oracle-health-suffers-major-breach-hospital-data-potentially-exposed.

[26] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

40. Plaintiff Shannon Smith is a current patient of Union Health.

41. Thus, Defendants obtained and maintained Plaintiff's PII/PHI.

42. As a result, Plaintiff was injured by Defendants' Data Breach.

43. Plaintiff is very careful about the privacy and security of his PII/PHI. He does not knowingly transmit his PII/PHI over the internet in an unsafe manner. He is careful to store any documents containing his PII/PHI in a secure location.

44. Plaintiff provided his PII/PHI to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

45. Plaintiff reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII/PHI.

46. Plaintiff received a Notice of Data Breach on April 29, 2025.

47. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

48. Through its Data Breach, Defendants compromised Plaintiff's PII/PHI.

49. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendants directed Plaintiff to take those steps in its breach notice.

50. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

51. Because of Defendants' Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

52. Plaintiff suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

53. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendants were required to adequately protect.

54. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

55. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

56. Today, Plaintiff has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Consumers Prioritize Data Security

57. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[27] Therein, Cisco reported the following:

[27] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[28]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[29]

c. 89% of consumers stated that "I care about data privacy."[30]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[31]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[32]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[33]

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

58. Because of Defendants' failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*,

[28] *Id*. at 3.
[29] *Id*.
[30] *Id*. at 9.
[31] *Id*.
[32] *Id*.
[33] *Id*. at 11.

monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendants' possession—and is thus as risk for futures breaches so long as Defendants fails to take appropriate measures to protect the PII/PHI.

59. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

60. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

61. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

62. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

63. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

64. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

65. Defendants disclosed the PII/PHI of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII/PHI of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

66. Defendants' failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them of the

earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants Knew—Or Should Have Known—of the Risk of a Data Breach

67. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

68. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[34] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[35] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[36]

69. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[37]

70. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[38]

---

[34] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.
[35] *Id*.
[36] *Id*.
[37] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[38] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

71. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendant.

Defendants Failed to Follow FTC Guidelines

72. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

73. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[39] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

74. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

75. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

[39] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

76. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

78. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

79. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

80. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

81. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

Defendants Violated HIPAA

82. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[40]

83. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[41]

[40] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[41] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

84. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security

incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

85. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

86. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Defendants in February 2025, including all those individuals who received notice of the breach.

87. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendants has a controlling interest, any Defendants officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

88. Plaintiff reserves the right to amend the class definition.

89. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

90. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendants' custody and control. After all, Defendants already identified some individuals and sent them data breach notices.

91. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 100 members.

92. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

93. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

94. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendants were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendants breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendants' Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

95. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of

scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

97. Plaintiff and the Class (or their third-party agents) entrusted their PII/PHI to Defendants on the premise and with the understanding that Defendants would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

98. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendants' failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

99. Defendants has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

100. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security practices. After all, Defendants actively sought and obtained Plaintiff and Class Members' PII/PHI.

101. Defendants owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

102. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

103. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

104. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

105. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendants with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

106. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendants hold vast amounts of PII/PHI, it was inevitable

that unauthorized individuals would attempt to access Defendants' databases containing the PII/PHI —whether by malware or otherwise.

107. PII/PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

108. Defendants improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

109. Defendants breached these duties as evidenced by the Data Breach.

110. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

111. Defendants breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

112. Defendants further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

113. Defendants has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

114. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

115. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

116. Defendants' breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

118. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII/PHI.

119. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC

publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the Class Members' sensitive PII/PHI.

120. Defendants breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

121. Defendants violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

122. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

123. But for Defendants' wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

124. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants were failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

125. Similarly, under HIPAA, Defendants had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class Members' PHI.

126. Defendants violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of PHI that Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

127. Defendants' various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

128. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

129. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

130. Plaintiff and Class Members either directly contracted with Defendants or Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendant.

131. Plaintiff and Class Members (or their third-party agents) were required to provide their PII/PHI to Defendants as a condition of receiving medical services provided by Defendant. Plaintiff and Class Members (or their third-party agents) provided their PII/PHI to Defendants or its third-party agents in exchange for Defendants' medical services.

132. Plaintiff and Class Members (or their third-party agents) reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

133. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were

required to provide based on Defendants' duties under state and federal law and its internal policies.

134. Plaintiff and the Class Members (or their third-party agents) accepted Defendants' offers by disclosing their PII/PHI to Defendants or its third-party agents in exchange for medical services.

135. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII/PHI to unauthorized persons.

136. In its Privacy Policy, Defendants represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

137. Implicit in the parties' agreement was that Defendants would provide Plaintiff and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

138. After all, Plaintiff and Class Members (or their third-party agents) would not have entrusted their PII/PHI to Defendants (or their third-party agents) in the absence of such an agreement with Defendant.

139. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

140. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

141. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

142. Defendants materially breached the contracts it entered with Plaintiff and Class Members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendants created, received, maintained, and transmitted.

143. In these and other ways, Defendants violated its duty of good faith and fair dealing.

144. Defendants' material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

145. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

146. Plaintiff and Class Members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

147. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

148. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

149. Defendants owed a duty to its current and former patients, including Plaintiff and the Class, to keep this information confidential.

150. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII/PHI is highly offensive to a reasonable person.

151. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

152. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

153. Defendants acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

154. Defendants acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

155. Acting with knowledge, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

156. As a proximate result of Defendants' acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

157. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

158. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendants with their inadequate cybersecurity system and policies.

159. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the PII/PHI of Plaintiff and the Class.

160. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

161. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

162. This claim is pleaded in the alternative to the breach of implied contract claim.

163. Plaintiff and Class Members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendants benefitted from (1) using their PII/PHI to provide services and (2) accepting payment.

164. Defendants appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

165. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

166. Defendants enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII/PHI.

167. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

168. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII/PHI and (2) payment because Defendants failed to adequately protect their PII/PHI.

169. Plaintiff and Class Members have no adequate remedy at law.

170. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

171. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

172. Given the relationship between Defendants and Plaintiff and Class Members, where Defendants became guardian of Plaintiff's and Class Members' PII/PHI, Defendants became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII/PHI; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

173. Defendants has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendants' relationship with them—especially to secure their PII/PHI.

174. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendants' position, to retain their PII/PHI had they known the reality of Defendants' inadequate data security practices.

175. Defendants breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII/PHI.

176. Defendants also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

177. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

178. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

179. Plaintiff and Class Members disclosed their highly sensitive PII/PHI to Defendants in confidence—with the implicit and explicit understanding that Defendants would collect, store, and protect their PII/PHI (and *not* allow the disclosure of their PII/PHI to unauthorized third parties).

180. As such, by obtaining (and continuing to maintain) Plaintiff's and Class Members' PII/PHI, Defendants assumed an obligation to maintain the confidentiality of that PII/PHI.

181. At all times during the relationship between Defendants and Plaintiff and Class Members, Defendants were fully aware of the highly confidential nature of Plaintiff's and Class Members' PII/PHI.

182. Thus, Defendants intentionally, knowingly, and/or negligently committed the tort of breach of confidence by, *inter alia*:

a. failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII/PHI;

b. failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period;

c. and via the numerous instances of misconduct detailed *supra*.

183. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

EIGHTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

184. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

185. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

186. In the fallout of the Data Breach, an actual controversy has arisen about Defendants' various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendants' actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

187. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendants has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendants breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

188. The Court should also issue corresponding injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the data entrusted to it.

189. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendants experiences a second data breach.

190. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class Members' injuries.

191. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

192. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendants and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: May 6, 2025

Respectfully submitted,

By: /s/ *John F. Garvey*
John F. Garvey, #35879
Colleen Garvey, #72809
STRANCH, JENNINGS & GARVEY, PLLC
St. Louis, Missouri 63101
Telephone: (314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com

Lynn A. Toops*
Amina A. Thomas*
One Indiana Square, Suite 1400
Indianapolis, IN 46204
T: (317) 636-6481
F: (317) 636-2593
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

**Pro hac vice forthcoming*
Attorneys for Plaintiff and Proposed Class

EXHIBIT A

Union Health

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Shannon C Smith
[redacted]

April 21, 2025

Dear Shannon C Smith,

We are writing to inform you about a security incident at Cerner, which is now part of Oracle Health ("Oracle Health/Cerner"), a third-party electronic health records ("EHR") vendor used by Union Health affiliates, including Union Hospital, Inc. and Union Medical Group (collectively "Union Health"). This notice explains the Oracle Health/Cerner incident, outlines the measures we have taken in response, and offers steps you can take.

What Happened?
An unknown party contacted Union Health claiming they had some patient information in their possession, which we verified on February 24, 2025. Union Health then identified the information as likely relating to data migration services performed by Oracle Health/Cerner, and proactively reached out to Oracle Health/Cerner for confirmation. We also immediately began an investigation with the assistance of cybersecurity specialists and notified law enforcement.

On March 15, 2025, Oracle Health/Cerner informed Union Health that it did have a cybersecurity event involving unauthorized access to data hosted in Oracle Health/Cerner's data migration environment. Oracle Health/Cerner further informed us that, on February 20, 2025, they first became aware of the incident and that their investigation identified the unauthorized party's initial access as taking place sometime after January 22, 2025. On March 22, 2025, Oracle Health/Cerner provided us with a list of Union Health patients whose information was involved.

It is important to note that the incident occurred on Oracle Health/Cerner's system, *not* Union Health's systems. In other words, this incident did not involve access to, or a compromise of, any Union Health owned, operated or administered systems, including Union Health's live EHR.

What Information Was Involved?
Per Oracle Health/Cerner, the files involved in the incident contained information that varied per patient but could have included your name and one or more of the following: Social Security number, driver's license number, date of birth, treating physician, dates of service, medication information, insurance information and treatment and/or diagnostic information.

What We Are Doing & What You Can Do.
While the incident did not impact Union Health's own network, we are notifying you of this incident and sharing the steps that we are taking in response. We remain committed to upholding high standards of custodianship of Union Health information held by our third-party vendors, including Oracle Health/Cerner.

We are also offering a complimentary 12-month membership of Experian's IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides identity protection services focused on identification and resolution of identity theft. IdentityWorks℠ Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks℠ Credit 3B, including instructions on how to activate your complimentary membership, please see the additional information provided with this letter.

For More Information.
We regret any concern that this incident may cause you, and we continue to review and assess the cybersecurity protections of our third-party vendors. Should you have any further questions regarding this matter, please do not hesitate to call 1-888-562-7131, Monday through Friday, between 9:00 am and 9:00 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Union Health

Activate IdentityWorks Credit 3B Now in Three Easy Steps

ROLL by: **July 31, 2025** (Your code will not work after this date.)
SIT the **Experian IdentityWorks website** to enroll: **www.experianidworks.com/3bcredit**
ROVIDE the **Activation Code: MKQM2QVQC7**

ve questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian Works online, please contact Experian's customer care team at 833-918-7223 by **July 31, 2025**. Be prepared to provide nent number **B144056** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

dit card is not required for enrollment in Experian IdentityWorks Credit 3B.

can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration ialists are available to help you address credit and non-credit related fraud.

ce you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers

ou believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issue se reach out to an Experian agent at 833-918-7223. If, after discussing your situation with an agent, it is determined that Identi toration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve ea dent of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and cl ounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contact vernment agencies to help restore your identity to its proper condition).

ase note that this Identity Restoration support is available to you for one year from the date of this letter and does not require tion on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. ll also find self-help tips and information about identity protection at this site.

Offline members will be eligible to call for additional reports quarterly after enrolling.

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Ass ompany. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available *risdictions.*

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/. Union Health can be reached by mail at 1606 North 7th Street, Terre Haute, IN 47804 or by phone at (812) 238-7000.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov. Union Health can be reached by mail at 1606 North 7th Street, Terre Haute, IN 47804 or by phone at (812) 238-7000.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 4 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

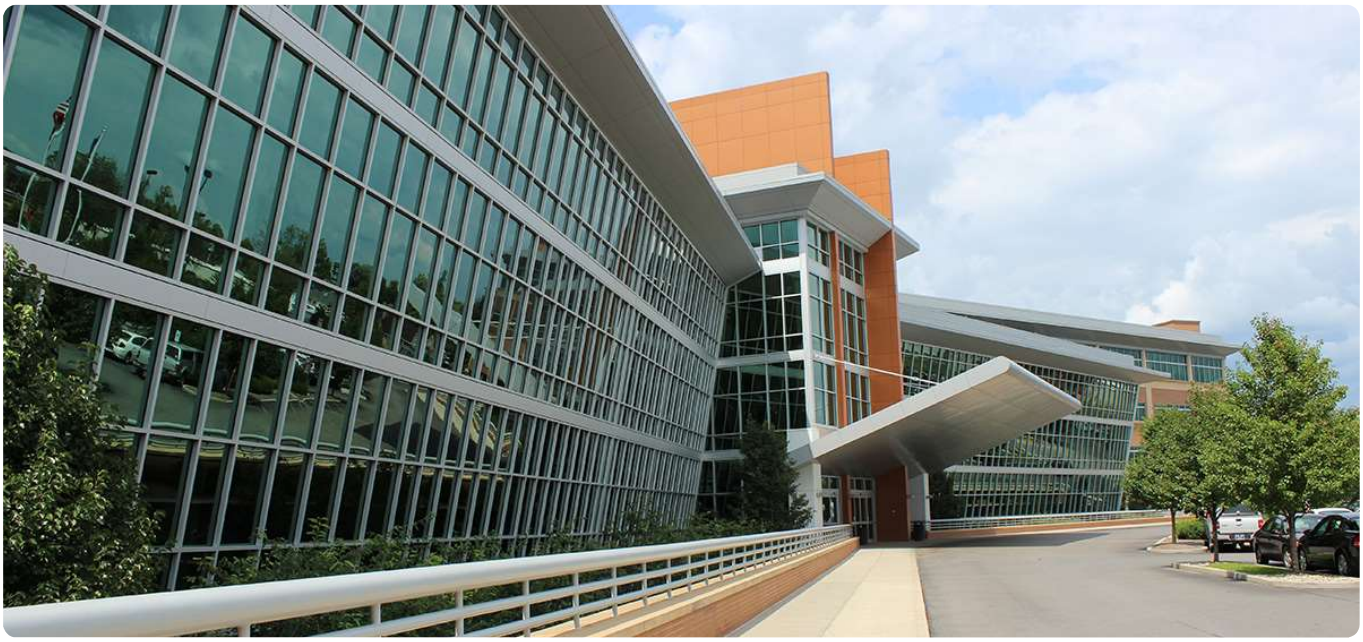
After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

EXHIBIT B

Notice of Oracle Health/Cerner Data Security Incident



Monday, April 21, 2025

On April 21, 2025, Union Health affiliates, including Union Hospital, Inc. and Union Medical Group (collectively "Union Health") mailed notification letters to certain Union Health patients whose personal information was involved in the Oracle Health/Cerner incident.

An unknown party contacted Union Health claiming they had some patient information in their possession, which we verified on February 24, 2025. Union Health then identified the information as likely relating to data migration services performed by Oracle Health/Cerner, and proactively reached out to Oracle Health/Cerner for confirmation. We also immediately began an investigation with the assistance of cybersecurity specialists and notified law enforcement.

On March 15, 2025, Oracle Health/Cerner informed Union Health that it did have a cybersecurity event involving unauthorized access to data hosted in Oracle Health/Cerner's data migration environment. Oracle Health/Cerner further informed us that, on February 20, 2025, they first became aware of the incident and that their investigation identified the unauthorized party's initial access as taking place sometime after January 22, 2025. On March 22, 2025, Oracle Health/Cerner provided us with a list of Union Health patients whose information was involved.

It is important to note that the incident occurred on Oracle Health/Cerner's system, *not* Union Health's systems. In other words, this incident did not involve access to, or a compromise of, any Union Health owned, operated or administered systems, including Union Health's live EHR.

Per Oracle Health/Cerner, the files involved in the incident contained information that varied per patient but could have included patients' names and one or more of the following: Social Security numbers, driver's license numbers, dates of birth, treating physicians, dates of service, medication information, insurance information and treatment and/or diagnostic information.

While the incident did not impact Union Health's own network, we are notifying patients of this incident and sharing the steps that we are taking in response. We remain committed to upholding high standards of custodianship of Union Health information held by our third-party vendors, including Oracle Health/Cerner. Union Health is offering complimentary identity monitoring services to patients. Additionally, it is always a good idea for patients to review statements they receive related to their healthcare provider or health insurer. If they identify charges for services they did not receive, they should contact the healthcare entity or health insurer immediately.

We also established a dedicated, toll-free call center to help answer questions about the data incident. The call center can be reached at 1-888-562-7131, Monday through Friday, between 9:00 am and 9:00 pm Eastern Time, excluding major U.S. holidays.

Search News...

Most Recent News


Apr 21 2025
Notice of Oracle Health/Cerner Data Security Incident


Mar 06 2025
Diabetes Care Moves to One Location


Feb 24 2025
Convenient Care Downtown Extends Hours

Contact Us

News Administrator

Healthier, together.


Shin Splints: Prevention and Treatment, Simplified


Recovery After Open Heart Surgery: What You Should Know


Snapping Hip: Why It Happens And What You Can Do About It


Common Heart Rhythm Disorders: Symptoms And Treatment

BACK TO TOP

OUR HEALTH SYSTEM

Union Health
Healthier, together.

JS 44 (Rev 09/10)

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI

CIVIL COVER SHEET

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the Western District of Missouri.

The completed cover sheet must be saved as a pdf document and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s):

First Listed Plaintiff:
Shannon Smith ;
2 Citizen of Another State; Indiana
County of Residence: Outside This District

Defendant(s):

First Listed Defendant:
Cerner Corporation d/b/a Oracle Health, Inc. ;
1 Citizen of This State;
County of Residence: Jackson County

Additional Defendants(s):
Union Health System, Inc. ;
2 Citizen of Another State; Indiana

County Where Claim For Relief Arose: Jackson County

Plaintiff's Attorney(s):

John F. Garvey (Shannon Smith)
Stranch, Jennings & Garvey, PLLC
701 Market Street
Saint Louis, Missouri 63101
Phone: 3143906750
Fax:
Email: jgarvey@stranchlaw.com

Defendant's Attorney(s):

Basis of Jurisdiction: 4. Diversity of Citizenship

Citizenship of Principal Parties (Diversity Cases Only)

Plaintiff: 2 Citizen of Another State

Defendant: 1 Citizen of This State

Origin: 1. Original Proceeding

Nature of Suit: 190 All Other Contract Actions
Cause of Action: 28 U.S.C. §1332 (d)(2).
Requested in Complaint

Class Action: Class Action Under FRCP23

Monetary Demand (in Thousands):

Jury Demand: Yes

Related Cases: Is NOT a refiling of a previously dismissed action

---

Signature: /s/ John F. Garvey

Date: 5/6/2025

If any of this information is incorrect, please close this window and go back to the Civil Cover Sheet Input form to make the correction and generate the updated JS44. Once corrected, print this form, sign and date it, and submit it with your new civil action.